بسم الله الرحمان الرحيم

السلام عليكم و رحمة الله تعالى و بركاته، أما بعد لن أطيل عليكم بالكلام لأنني من الناس الذين يتكلمون قليلا و يفهمون كثيرا إن شاء الله، لأهمية هذا الموضوع قمت بنشر هذا الكتيب للاستفادة الجماعية .

هدفي من كتابة هذا الموضوع المدعم بالصور العديدة هو توفير أقصى درجة من الحماية لجميع مستخدمي الكمبيوتر و لا تتعجبوا لكثرة الصور ،و ذلك لأسباب عديدة أهمها هو أنكم عندما تشاهون الصور ستدركون مدى خطورة الهاكرز .

ملاحظة : أي أحد يحصل على هذا الكتيب من فضله أن يقوم بنشره لشخص آخر شريطة عدم إستغلاله في أي غرض تجاري لتعم الفائدة على الجميع .

الفهرس :

نبذة عن الكاتب

الإسم : عدلان الملقب **بالصقر الجارح**

من مواليد 17 نوفمبر 1991 هو الآن يدرس في الثانوية

السكن : الجزائر – عنابة

الهواية : البرمجة بلغة فيجوال و سي كما سبق و تتطرق الى لغات تطوير المواقع

مشجع فريق إتحاد مدينة عنابة و البارصا



الهاكينغ أو التجسس

تسمى باللغة الإنجليزية Hacking و بالغة العربية عملية التجسس أو الاختراق..

حيث يقوم أحد الأشخاص الغير مصرح لهم بالدخول إلى نظام التشغيل في جهازك بطريقة غير شرعية ولأغراض غير سوية مثل التجسس أو السرقة أو التخريب حيث يتاح للشخص المتجسس (الهاكر) أن ينقل أو يمسح أو يضيف ملفات أو برامج كما أنه بإمكانه أن يتحكم في نظام التشغيل فيقوم بإصدار أوامر مثل إعطاء أمر الطباعة أو التصوير أو التخزين..

من هم الهاكرز ؟

هم الأشخاص الذين يخترقون جهازك فيستطيعون مشاهدة ما به من ملفات أو سرقتها أو تدمير جهازك أو التلصص ومشاهدة ما تفعله على شبكة الإنترنت..

ما هي الأشياء التي تساعدهم على إختراق جهازك ؟

في غالب الأحيان يحتاج الهاكر الى ثلاثة أشياء رئيسية :

- ✓ الباتش أو التروجان

لا يستطيع الهاكر الدخول إلى جهازك إلا مع وجود ملف يسمى Patch أو Trojan في جهازك وهذه الملفات هي التي يستطيع الهاكر بواسطتها الدخول إلى جهازك الشخصي حيث يستخدم الهاكر أحد برامج التجسس التي ترتبط مع ملف الباتش الذي يعمل ك (ريسيفر) يستطيع أن يضع له الهاكر (إسم مستخدم) و (رمز سري) تخوله أن يكون هو الشخص الوحيد الذي يستطيع الدخول إلى جهازك وكذلك يستطيع أن يجعل جهازك مفتوحاً فيستطيع أي هاكر أن يدخل إلى جهازك!!

- ✓ الاتصال بشبكة الإنترنت

لا يستطيع الهاكر أن يدخل إلى جهازك إلا إذا كنت متصلاً بشبكة الإنترنت أما إذا كان جهازك غير متصل بشبكة الإنترنت أو أي شبكة أخرى فمن المستحيل أن يدخل أحد إلى جهازك سواك !!
ولذلك إذا أحسست بوجود هاكر في جهازك فسارع إلى قطع الاتصال بخط الإنترنت بسرعة حتى تمنع الهاكر من مواصلة العبث والتلصص في جهازك..

- ✓ برنامج التجسس

حتى يتمكن الهاكر العادي من إختراق جهازك لابد أن يتوافر معه برنامج يساعده على الاختراق!

ومن أشهر برامج الهاكرز هذه البرامج

Back orifice
Deep Throat Remote
Doly Trojan
Net Bus 1.7
Girl Friend
Sockets de Troie
Acid Shivers
Netsphere
Win crash
Blad runner

كيف يتمكن الهاكر من الدخول إلى جهازك ؟

عندما يتعرض جهاز الكمبيوتر للإصابة بملف التجسس وهو (الباتش أو التروجان) فإنه على الفور يقوم بفتح بورت (port) أو منفذ داخل جهازك فيستطيع كل من لديه برنامج تجسس أن يقتحم جهازك من خلال هذا الملف الذي يقوم بفتح منطقة أشبه بالنافذة السرية التي يدخل منها اللصوص وهم الهاكرز!!

كيف يتمكن الهاكر من الدخول إلى جهاز كمبيوتر بعينه ؟

لا يستطيع الهاكر أن يخترق جهاز كمبيوتر بعينه إلا إذا توافرت عدة شروط أساسية وهي :

- إحتواء كمبيوت الضحية على ملف التجسس PATCH
- إذا كان الهاكر يعرف رقم الآي بي أدرس الخاص بهذا الشخص .. وطبعاً لابد من وجود الشروط الأخرى وهي إتصال الضحية بالإنترنت ومعرفة الهاكر بكيفية إستخدام برنامج التجسس والاختراق من خلاله.

بمعنى آخر إذا كان جهاز الكمبيوتر سليماً ولا يحوي أي ملفات باتش فمن المستحيل أن يدخل عليه أي هاكر عادي حتى لو كان يعرف رقم الآي بي أدرس ما عدا المحترفين فقط وهم قادرون على الدخول بأية طريقة وتحت أي مانع ولديهم طرقهم السرية في الولوج إلى مختلف الأنظمة !!

وإذا كان الهاكر لا يعرف رقم الآي بي أدرس الخاص بك فإنه لن يستطيع الدخول إلى جهازك حتى لو كان جهازك يحوي ملف الباتش !

رقم ال IP Adress

هو العنوان الخاص بكل مستخدم لشبكة الإنترنت أي أنه الرقم الذي يُعَرف مكان الكمبيوتر أثناء تصفح شبكة الإنترنت وهو يتكون من 4 أجزاء وكل جزء منها يشير إلى عنوان معين فأحدها يشير إلى عنوان البلد والتالي يشير إلى عنوان الشركة الموزعة والثالث إلى المؤسسة المستخدمة والرابع هو المستخدم.

ورقم الآي بي متغير وغير ثابت فهو يتغير مع كل دخول إلى الإنترنت .. بمعنى آخر لنفرض أنك إتصلت بالانترنت ونظرت إلى رقم الآى بي الخاص بك فوجدت أنه : 212.123.123.200

ثم خرجت من الانترنت أو أقفلت الاتصال ثم عاودت الاتصال بعد عدة دقائق فإن الرقم يتغير ليصبح كالتالي: 212.123.123.366

لاحظ التغير في الأرقام الأخيرة : الرقم 200 أصبح 366 .
ولذلك ينصح بعدم استخدام بعرض برامج المحادثة مثل الآيسكيو ICQ لأنه يقوم بإظهار رقم الآي بي بشكل دائم حتى مع إخفائه فيتمكن الهاكر من استخدامه في الدخول إلى جهاز الشخص المطلوب مع توافر شرط وهو أن يحتوي كمبيوتر هذا الشخص على منفذ أو ملف تجسس PATCH

كيف يصاب جهازك بملف الباتش أو التروجان أو حتى الفيروسات ؟

هناك عدة طرق يمكن بسببها أن يصاب الكمبيوتر بهذه الشوائب :

- الطريقة الأولى :

أن يصلك ملف التجسس من خلال شخص عبر المحادثة أو (الشات) وهي أن يرسل أحد الهاكر لك صورة أو ملف يحتوي على الباتش أو التروجان!
ولابد أن تعلم صديقي العزيز أنه بإمكان الهاكر أن يغرز الباتش في صورة أو ملف فلا تستطيع معرفته إلا باستخدام برنامج كشف الباتش أو الفيروسات حيث تشاهد الصورة أو الملف بشكل طبيعي ولا تعلم أنه يحتوي على باتش أو فيروس ربما يجعل جهازك عبارة عن شوارع يدخلها الهاكر والمتطفلون !

- الطريقة الثانية :

أن يصلك الباتش من خلال رسالة عبر البريد الإلكتروني لا تعلم مصدر الرسالة ولا تعلم ماهية الشخص المرسل فتقوم بتنزيل الملف المرفق مع الرسالة ومن ثم فتحه وأنت لا تعلم أنه سيجعل الجميع يدخلون إلى جهازك ويتطفلون عليك .

- الطريقة الثالثة :

إنزال برامج أو ملفات من مواقع مشبوهة مثل المواقع الاباحية أو المواقع التي تساعد على تعليم التجسس!

- الطريقة الرابعة :

الدخول إلى مواقع مشبوهة مثل المواقع الاباحية حيث أنه بمجرد دخولك إلى الموقع فإنه يتم تنزيل الملف في جهازك بواسطة كوكيز لا تدري عنها!!

كيف يختار الهاكر الجهاز الذي يود إختراقه ؟

بشكل عام لا يستطيع الهاكر العادي من اختيار كمبيوتر بعينه لاختراقه إلا إذا كان يعرف رقم الآي بي أدرس الخاص به كما ذكرنا سابقاً فإنه يقوم بإدخال رقم الآي بي أدرس الخاص بكمبيوتر الضحية في برنامج التجسس ومن ثم إصدار أمر الدخول إلى الجهاز المطلوب . وأغلب المخترقين يقومون باستخدام برامج الكشف عن رقم الأيبي مثل IP Scanner و Any IP tracer و UltraScan

من ثم يحصلون على المنافذ المفتوحة أي الأجهزة المضروبة بأي ملف تجسس **PATCH**

يتم تشغيل البرنامج ثم يقوم المخترق بوضع أرقام آَي بي إفتراضيه .. أي أنه يقوم بوضع رقمين مختلفين فيطلب من الجهاز البحث بينهما فمثلاً يختار هذين الرقمين :

212.224.123.10

212.224.123.100

لاحظ آخر رقمين وهما : 10 و 100 ، فيطلب منه البحث عن كمبيوتر يحوي منفذ (كمبيوتر مضروب) بين أجهزة الكمبيوتر الموجودة بين رقمي الآَي بي أدرس التاليين : 212.224.123.10 و 212.224.123.100 وهي الأجهزة التي طلب منه الهاكر البحث بينها

بعدها يقوم البرنامج بإعطائه رقم الآَي بي الخاص بأي كمبيوتر مضروب يقع ضمن النطاق الذي تم تحديده مثل :

212.224.123.50

212.224.123.98

212.224.123.33

212.224.123.47

فيخبره أن هذه هي أرقام الآَي بي الخاصة بالأجهزة المضروبة التي تحوي منافذ أو ملفات تجسس فيستطيع الهاكر بعدها من أخذ رقم الآَي بي ووضعه في برنامج التجسس ومن ثم الدخول إلى الأجهزة المضروبة!

أشهر برامج الهاكرز

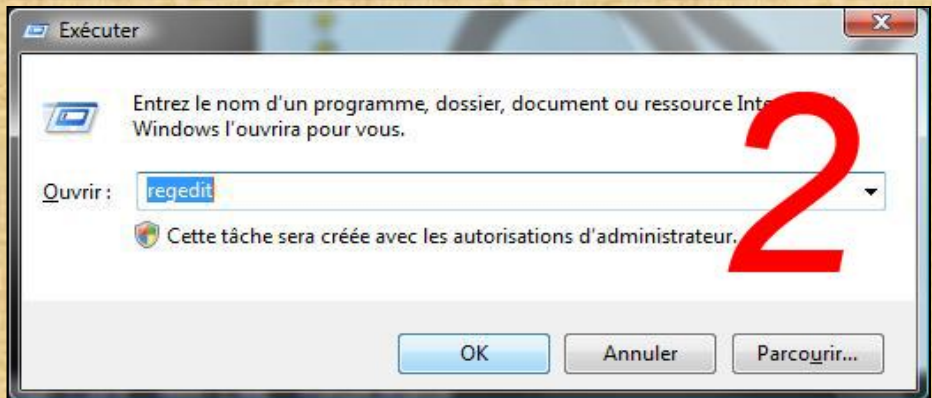
Netbus1.70

من أقدم البرامج في ساحة الاختراق بالسيرفرات وهو الأكثر شيوعا بين مستخدمي المايكروسوفت شات وهو برنامج به العديد من الإمكانيات التي تمكن الهاكر من التحكم بجهاز الضحية وتوجد نسخ مختلفة أكثر حداثة من النت باس وكل نسخى منها أكثر تطوراً من الأخرى، و لوجوده إذهب الى الامتداد التالي :

(HKEY_LOCAL_MACHINE\Software\Microsoft\windows\currentversion\run)

في الروجيستري Regedit، إظغط على Demmarer\exécuter\regedit





عندما تذهب الى المسار السابق ستجد ملف اسمه (PATCH.EXE) سواء في الروجيستري أو في الفولدر System قم بحذفه مباشرة .

البورتات التي يتسلل منها هي (12345) (12346)

SUB 7

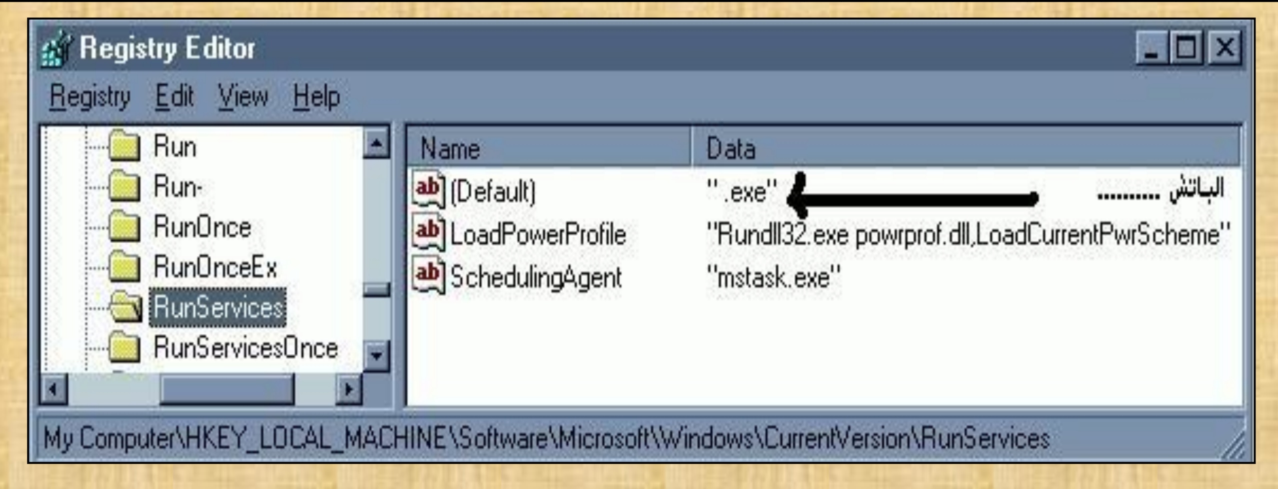
برنامج ممتاز وغني عن التعريف .. تستطيع التحكم وتنسيق السيرفر ليعمل كيفما تشاء سواء من تغيير شكل او طريقة عمل وهو ممتاز في مجال الاختراق بالبرامج

Hackers Utility

برنامج مفيد ورهيب للهاكرز وخاصة المبتدئين والمحترفين حيث أنه يمتلك أغلب وأفضل إمكانيات مختلف برامج الهاكرز ويمكن من خلاله كسر الكلمات السرية للملفات المضغوطة وفك تشفير الملفات السرية المشفرة وكذلك تحويل عناوين المواقع الى أرقام آي بي والعكس كما به العديد العديد من الإمكانيات والمميزات التي يبحث عنها الكثير من الهاكرز .

Back Orifice

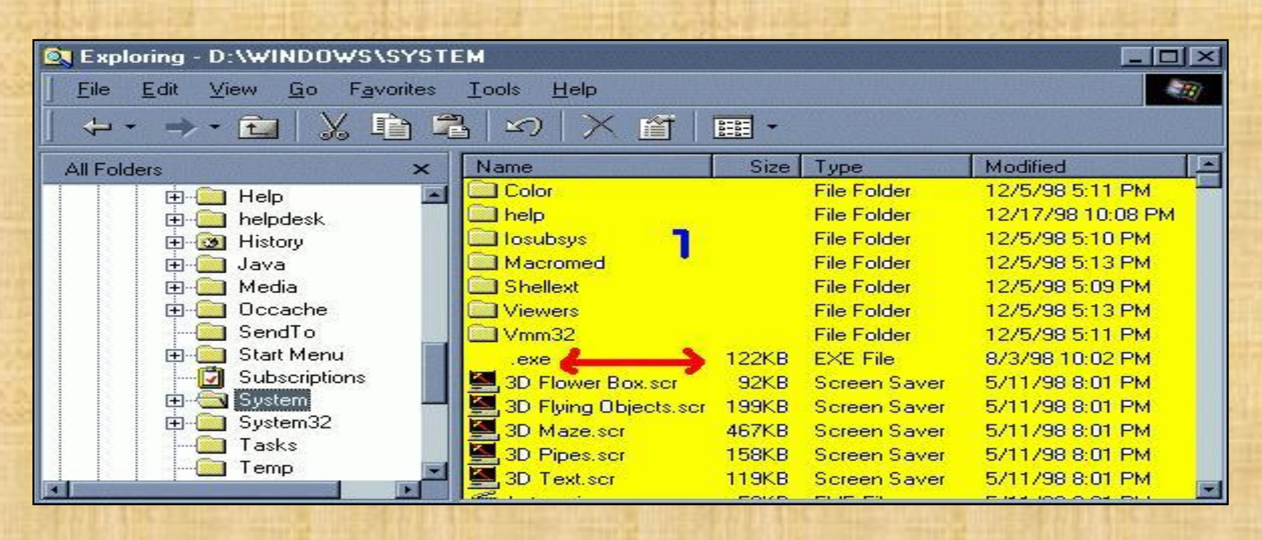
برنامج غني عن التعريف حيث يعتبر من أقوى و أخبث برامج الاختراق،قوي في التعامل مع الضحية و مفعوله سريع جدا ،غير أن عيبه الوحيد أنه عندما يريد الهاكر إختراق أحد الأجهزة يجب عليه أن يكون جهازه ملوث بالباتش نفسه الذي يستعمل للاختراق .

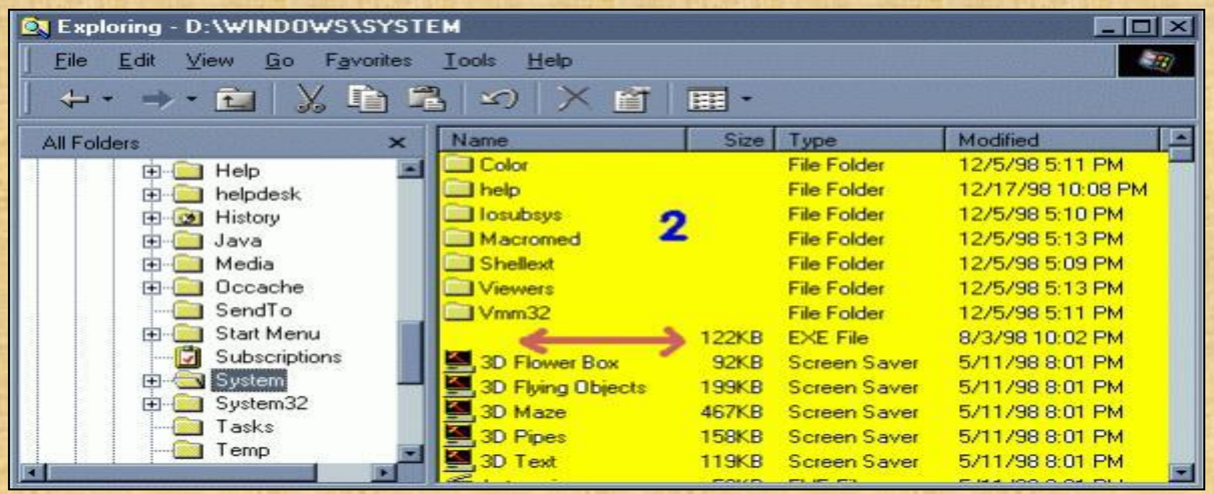


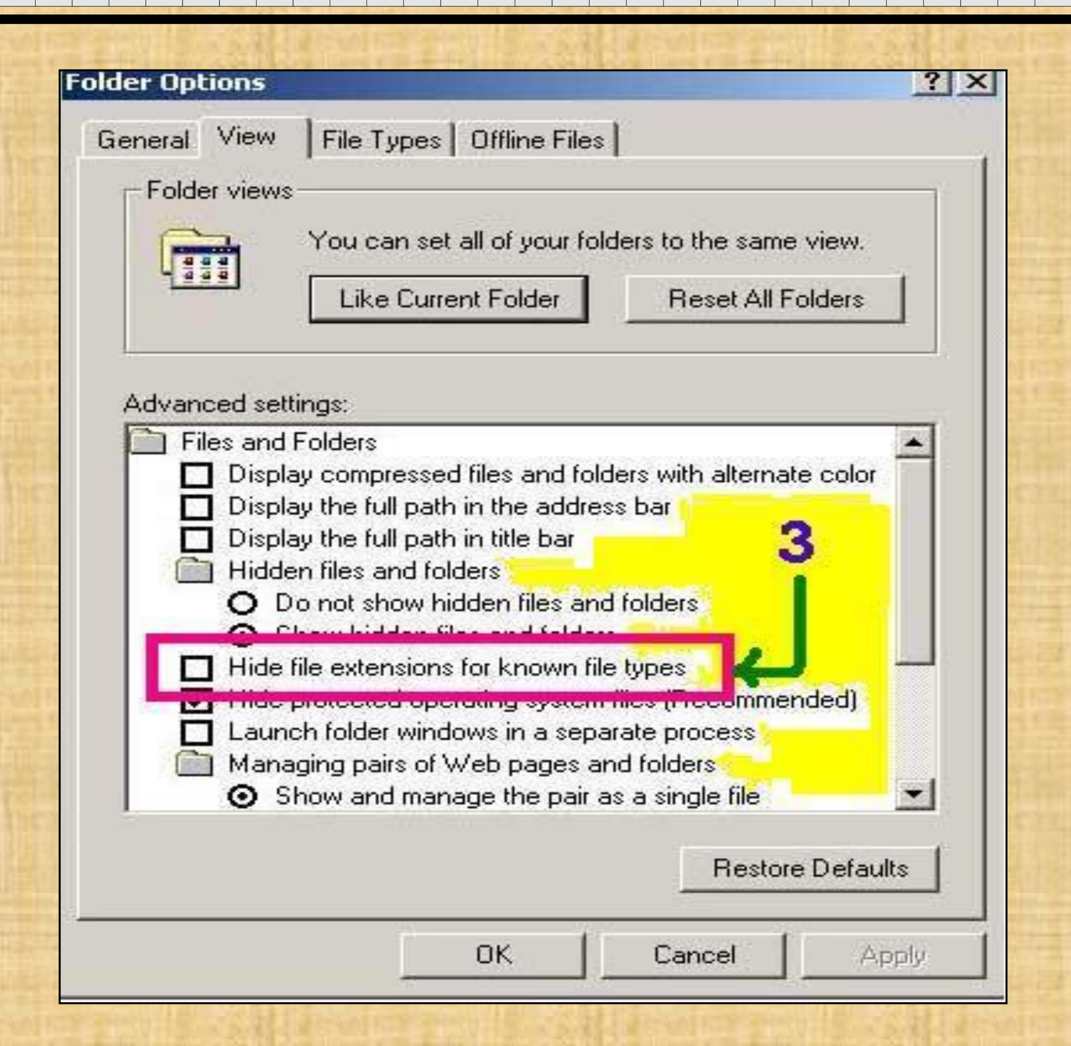
بالنسبة لتفسير الصورة السابقة فهو كالتالي ، غالبا و مع الأسف ما يكون ملف الباتش ليس له إسم أو مخفي و لكي تعرف مكانه ما عليكَ إلا الذهاب الى المسار التالي :

(HKEY_LOCAL_MACHINE\Software\Microsoft\windows\currentversion\runservices)

و عندما تظغط على (runservices)،ستجد على اليمين ملف ليس له إسم و هو مكتوب كالتالي (.exe). و من المفروض أن هذا المكان في الروجيستري ليس من المسموح وجود أية ملفات فيه .







Deep Throat Remote



يقوم هذا البرنامج بمسح الملف   سيستري ويقوم باستبداله بالسيرفر الخاص به وهذا البرنامج فيه ميزة وهي أنك تستطيع   التحكم في المواقع اللي يزورها الضحية وتقوم بتوجيهه لأي مكان ترغب وبإمكان المتحكم غلق وفتح الشاشة وكذلك إستخدامه عن طريق برنامج الإف تي بي .

و لكي تعرف مكانه ما عليك إلا الذهاب الى المسار التالي :

(HKEY_LOCAL_MACHINE\Software\Microsoft\windows\currentversion\run)

عندما تظغط على Run ستجد على اليمين الباتش و اسمه (SystemDll32)

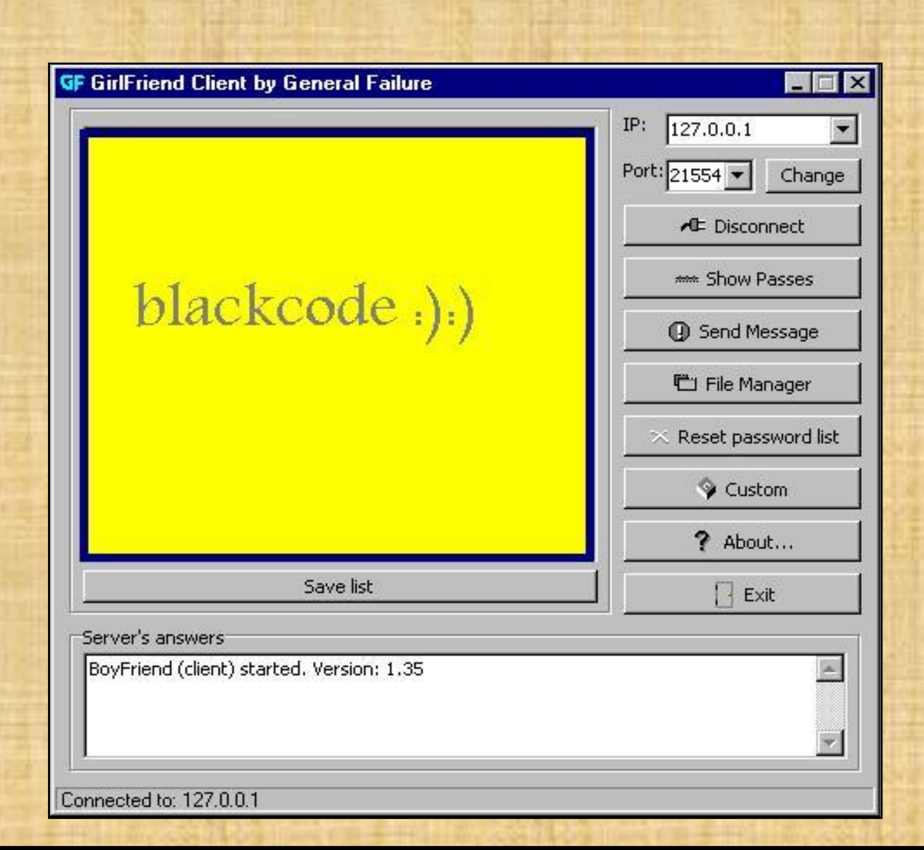
و طبعا لكي تزيل الباتش عليك بمسحه من المسار السابق مع العلم أنه هناك مف آخر في الويندوز و لكنه باسم (Systempatch.exe) عليك بمحوه .

أما بالنسبة للبورتات إتي يتسلل منها البرنامج هي : (2140) (3150) و هي من النوع (udp)

UltraScan

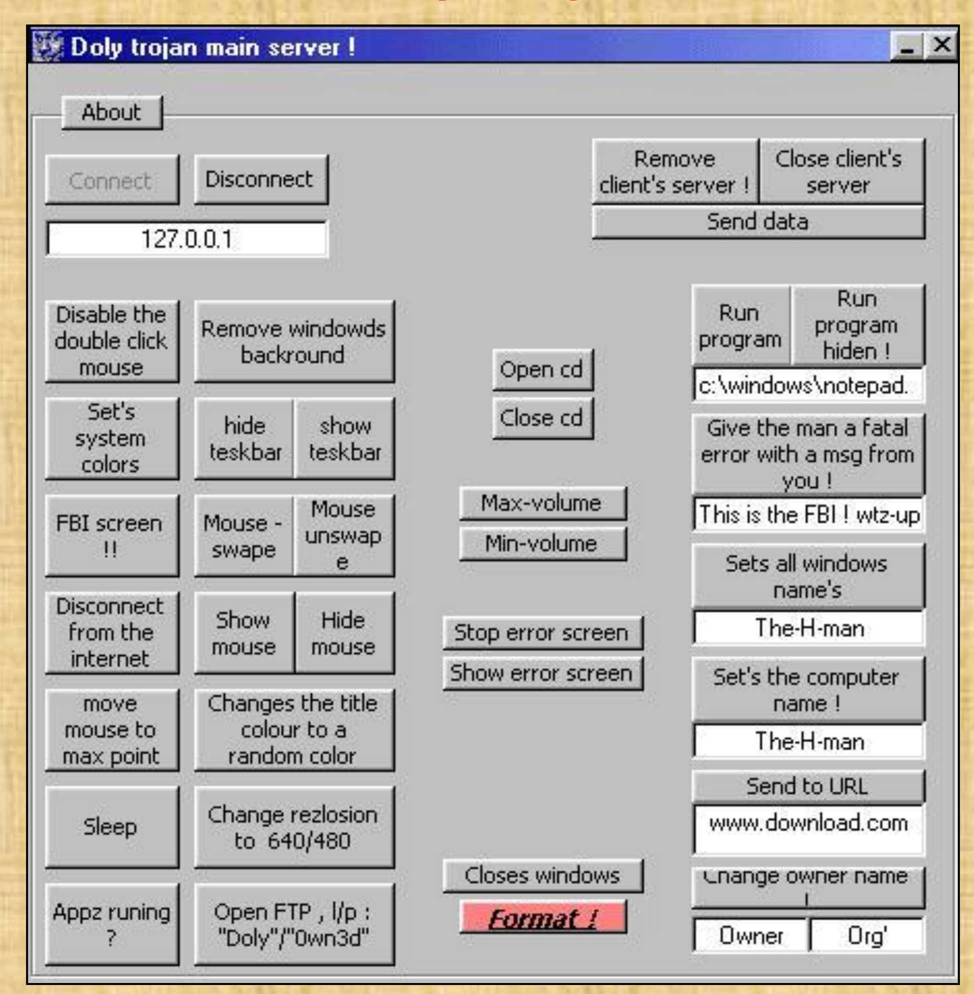
أسرع برنامج لعمل Scan على جهاز الضحية لمعرفة المنافذ المفتوحة التي يمكنك الدخول إليه منها...

Girl Friend



الرئيسية والخطيرة برنامج قام بعمله شخص يدعى بـــ(الفاشل العام) ومهمته الأيميل هي سرقة جميع كلمات السر الموجودة في جهازك بما فيها باسوورد وكذلك إسم المستخدم والرمز السري الذي تستخدمه لدخول الإنترنت .

Doly Trojan



برنامج رهيب في عملية الهيكرة ، و البورتات التي يتسلل منها البرنامج هي (1011)

كي تعرف مكان البرنامج ما عليك إلا إتباع المسار التالي :

(HKEY_LOCAL_MACHINE\Software\Microsoft\windows\currentversion\run)

و عندما تظغط على Run ستجد على اليمين باتش و اسمه (tesk.exe)

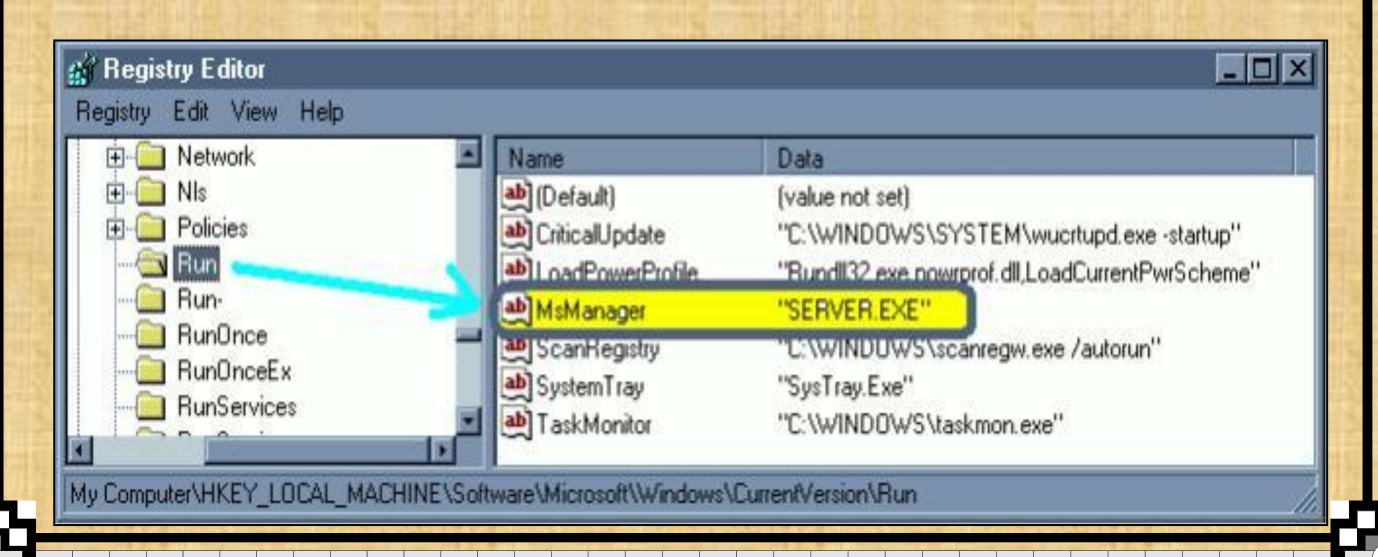
أو من الممكن أن تجده في هذا المسار أيضا و بنفس الاسم

(HKEY_LOCAL_USER\Software\Microsoft\windows\currentversion\run)

Wincrash

برنامج مفيد ورهيب للهاكرز وخاصة المبتدئين والمحترفين حيث أنه يمتلك أغلب وأفضل إمكانيات مختلف برامج الهاكرز ويمكن من خلاله فك تشفير الملفات السرية المشفرة وكذلك تحويل عناوين المواقع الى أرقام آي بي والعكس كما به العديد من الإمكانيات والميزات التي يبحث عنها الكثير من الهاكرز.

أما بالنسبة للبورتات التي يتسلل منها البرنامج هي : **(5742)**



كما رأيت في الصورة السابقة قم فورا بحذف الباتش MsMAnager .

كيف تعرف إذا كان جهازك مخترقاً أم لا ؟

في البداية تستطيع أن تعرف إذا كان جهازك مخترقاً من خلال معرفة التغيرات التي يحدثها الهاكرز في نظام التشغيل مثل فتح وغلق الشاشة تلقائياً أو وجود ملفات جديدة لم يدخلها أحد أو مسح ملفات كانت موجودة أو فتح مواقع إنترنت أو إعطاء أمر للطابعة بالإضافة إلى العديد من التغيرات التي تشاهدها وتعرفها وتعلم من خلالها عن وجود متطفل يستخدم جهازك.

هذه الطريقة تستطيع من خلالها أن تعرف هل دخل أحد المتطفلين إلى جهازك أم أن جهازك سليم منهم

إفتح قائمة (Demmarer) و منها إختر أمر (Exécuter)

إكتب التالي system.ini

ستظهر لك صفحة فاذهب للسطر الخامس فيها فإذا وجدت أن السطر مكتوب هكذا:

user. exe=user. Exe فاعلم أن جهازك لم يتم إختراقه من قبل الهاكرز.

أما إذا وجدت السطر الخامس مكتوب هكذا user. exe=user. exe *** *** ***

فاعلم أن جهازك قد تم إختراقه من أحد الهاكرز .

ما هي أهم الإحتياطات التي يجب إتخاذها للحماية من الهاكرز ؟

- إستخدم أحدث برامج الحماية من الهاكرز والفيروسات وقم بعمل مسح دوري وشامل على جهازك في فترات متقاربة خصوصاً إذا كنت ممكن يستخدمون الإنترنت بشكل يومي
- لا تدخل إلى المواقع المشبوهة مثل المواقع التي تعلم التجسس والمواقع التي تحارب الحكومات أو المواقع التي تحوي أفلاماً وصوراً خليعة لأن الهاكرز يستخدمون أمثال هذه المواقع في إدخال ملفات التجسس إلى الضحايا حيث يتم تنصيب ملف التجسس (الباتش) تلقائياً في الجهاز بمجرد دخول الشخص إلى الموقع!!

- عدم فتح أي رسالة إلكترونية من مصدر مجهول لأن الهاكرز يستخدمون رسائل البريد الإلكتروني لإرسال ملفات التجسس إلى الضحايا .
- عدم استقبال أية ملفات أثناء الشات من أشخاص غير موثوق بهم وخاصة إذا كانت هذه الملفات تحمل امتداد (exe) مثل (love.exe) أو أن تكون ملفات من ذوي الامتدادين مثل (adlene.pif.jpg) وتكون أمثال هذه الملفات عبارة عن برامج تزرع ملفات التجسس في جهازك فيستطيع الهاكرز بواسطتها من الدخول على جهازك وتسبيب الأذى والمشاكل لك.
- عدم الاحتفاظ بأية معلومات شخصية فى داخل جهازك كالرسائل الخاصة أو الصور الفوتوغرافية أو الملفات المهمة وغيرها من معلومات بنكية مثل أرقام الحسابات أو البطاقات الائتمانية
- قم بوضع أرقام سرية على ملفاتك المهمة حيث لا يستطيع فتحها سوى من يعرف الرقم السري فقط وهو أنت .
- حاول قدر الإمكان أن يكون لك عدد معين من الأصدقاء عبر الإنترنت وتوخى فيهم الصدق والأمانة والأخلاق .
- حاول دائماً تغيير كلمة السر بصورة دورية فهي قابلة للاختراق .
- تأكد من رفع سلك التوصيل بالإنترنت بعد الإنتهاء من استخدام الإنترنت.
- لا تقم بإستلام أي ملف وتحميله على القرص الصلب في جهازك الشخصي إن لم تكن متأكدا من مصدره

ما هي أهم الأشياء التي يبحث عنها الهاكرز ؟

بعض الهاكرز يمارسون التجسس كهواية وفرصة لإظهار الإمكانيات و استعراض العضلات البرمجية وتحدي الذات والبعض الآخر يمارس هذا العمل بدافع تحقيق عدة أهداف تختلف من هاكر لآخر ونذكر منها ما يلي:

- الحصول على المال من خلال سرقة المعلومات البنكية مثل أرقام الحسابات أو البطاقات الائتمانية
- الحصول على معلومات أو صور شخصية بدافع الابتزاز لأغراض مالية أو انحرافية كتهديد بعض الفتيات بنشر صورهن على الإنترنت إذا لم يستجبن لمطالب انحرافية أو مالية!!
- الحصول على ملفات جميلة مثل ملفات الأركامكس أو الباور بوينت أو الأصوات أو الصور أو...

- إثبات القدرة على الاختراق ومواجهة العقبات وفرصة للافتخار بتحقيق نصر في حال دخول الهاكر على أحد الأجهزة أو الأنظمة المعلوماتية
- الحصول على الرموز السرية للبريد الإلكتروني ليتسنى له التجسس على الرسائل الخاصة أو سرقة إسم البريد الإلكتروني بأكمله!
- الحصول على الرمز السري لأحد المواقع بهدف تدميره أو التغيير في محتوياته
- الانتقام من أحد الأشخاص وتدمير جهازه بهدف قهره أو إذلاله

ما هي أشهر طريقة للكشف عن ملفات التجسس ؟

هناك العديد من الطرق للكشف عن وجود ملفات التجسس في جهازك

الطريقة الأولى برامج الكشف عن ملفات التجسس والفيروسات

استخدام أحد برامج الكشف عن ملفات التجسس وكذلك الحماية من التجسس والهاكرز عن طريق عمل جدار ناري يمنع دخول المتطفلين ، من أشهر وأفضل برامج الكشف عن ملفات التجسس :

- Norton internet security
- Zone alarm
- MacAfee firewall
- The Cleaner
- Symantec endpoint protection 11
- Tiny Personal Firewall
- Jammer
- Kaspersky anti Hacker

الطريقة الثانية بواسطة ملف تسجيل النظام Registry

- انقر على زر البدء Demmarer
- أكتب في خانة التشغيل Exécuter الأمر Regedit
- افتح المجلدات التالية حسب الترتيب في قائمة Registery

(HKEY_LOCAL_USER\Software\Microsoft\windows\currentversion\run)

والآن من نافذة تسجيل النظام Editor Registry انظر الي يمين النافذة بالشاشة المقسومة ستشاهد تحت قائمة Names أسماء الملفات التي تعمل مع قائمة بدء التشغيل ويقابلها في قائمة Data عناوين الملفات

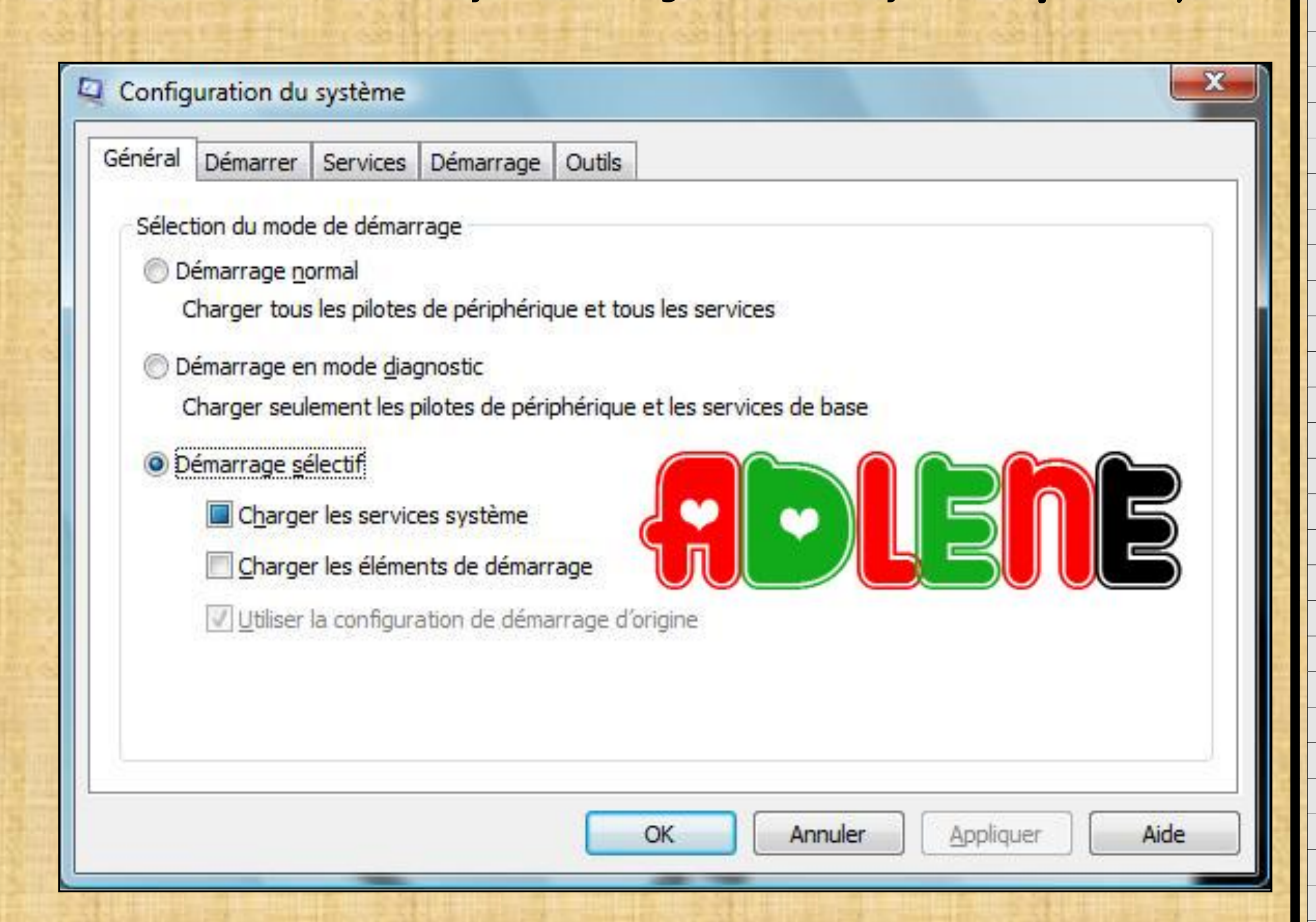
لاحظ الملفات جيدا فإن وجدت ملف لايقابلة عنوان بالـ Data او قد ظهر أمامة سهم صغير ---> فهو ملف تجسس إذ ليس له عنوان معين بالويندوز تخلص منه بالضغط على الزر الأيمن للفارة ثم Supprimer .

الطريقة الثالثة بواسطة الأمر Msconfig

- انقر على زر البدء Demmarer

-أكتب في خانة التشغيل Exécuter الأمر Msconfig

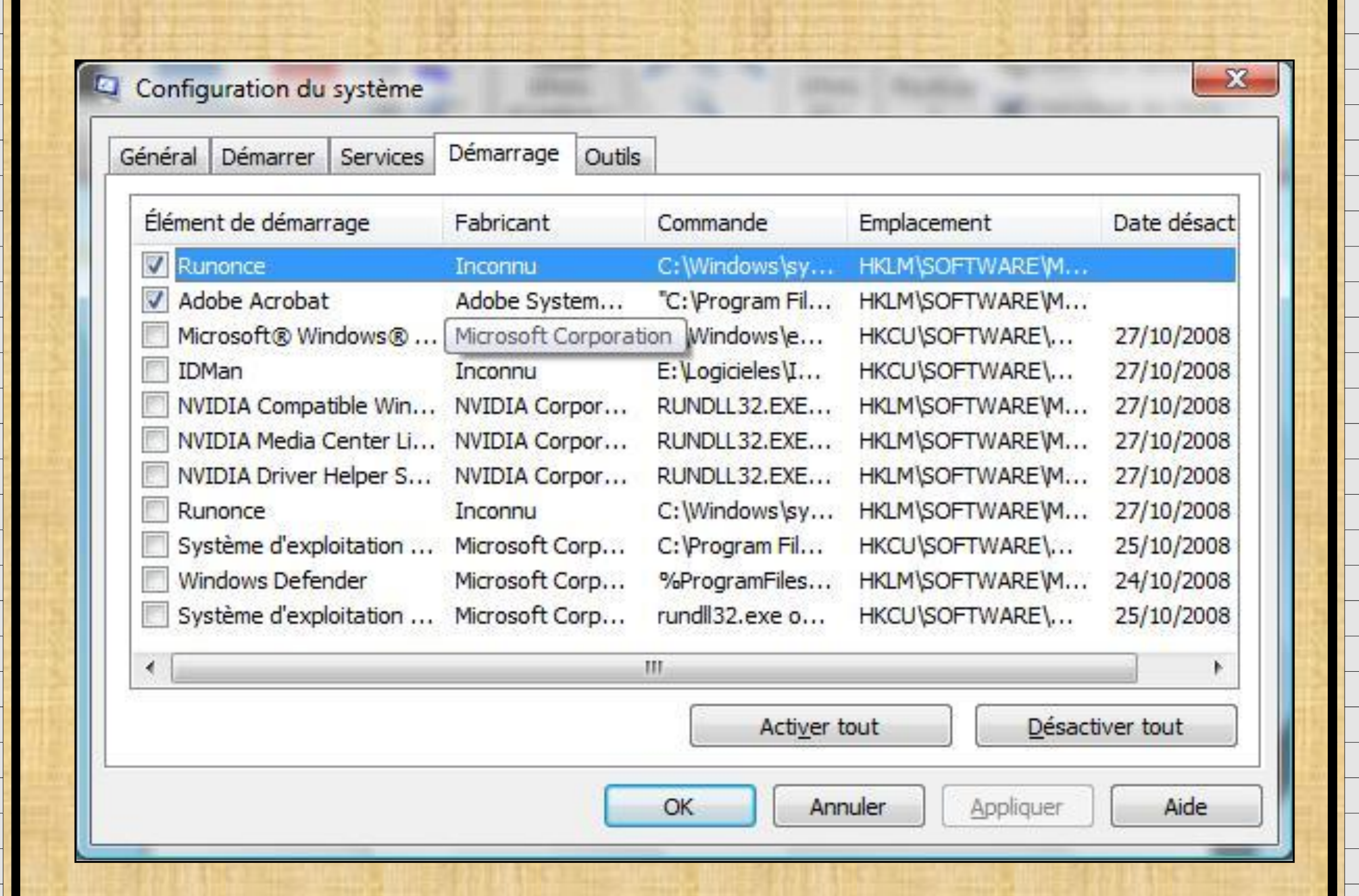
سوف تظهر لك نافذة System Configuration Utility



إختر من هذه النافذة من أعلى قسم Démarrage

ستظهر لك شاشة تعرض البرامج التي تبدأ العمل مباشرة مع بدء تشغيل الجهاز ، إفحص هذة البرامج جيدا بالنظر فإن شككت بوجود برامج غريبة لم تقم أنت

بتثبيتها بجهازك فقم بالغاء الإشارة الظاهرة بالمربع الصغير المقابل له فتكون بذلك قد أوقفت عمل البرنامج التجسسي أو غيره من البرامج الغير مرغوب بها



الطريقة الرابعة بواسطة مشغل الدوس MS DOS

هذة الطريقة كانت تستخدم قبل ظهور الويندوز لإظهار ملفات التجسس مثل الباتش والتروجانز وهي من اسهل الطرق

إفتح الدوس من محث MSDos بقائمة البدء Demmarer من ثم أكتب الأمر التالي

C:/Windows\dir patch.* e

إن وجدت ملف الباتش فقم بمسحة بالطريقة التالية C:\Windows\delete patch.*

مواقف مع الهاكرز

- أحد الهاكرز دخل على الجهاز الشخصي لإحدى الفتيات وأخذ يشاهد ما يحتويه من صور وملفات ولفت انتباهه أن الكاميرا موصلة بالجهاز

فأصدر أمر التصوير فأخذ يشاهدها وهي تستخدم الكمبيوتر ثم أرسل لها رسالة يخبرها فيها أنها جميلة جداً جداً ولكن يا ريت لو تقلل من كمية المكياج !!

- أحد الهاكرز المحترفين إعتاد أن يدخل على مواقع البنوك عبر الإنترنت ويتسلل بكل سلاسة إلى الأرصدة والحسابات فيأخذ دولار واحد من كل غني ويضع مجموع الدولارات في رصيد أقل الناس حساباً
- واحد من الشباب يدخل إلى أجهزة الناس ويقوم بحذف الصور الخليعة والملفات الاباحية ويعتبر نفسه بهذا مجرد فاعل خير وهو بهذا ينسى أنه حرامي ولص ومتسلل!
- إعتاد الهاكرز على محاولة إختراق المواقع الكبيرة مثل موقع الياهو وموقع مايكروسوفت ولكنهم دائماً ما يفشلون في مراميهم هذه بسبب الجدران النارية التي تضعها هذه الشركات والإجراءات الضخمة التي تتبعها لمنع أي هاكر من دخول النظام ومع هذا ينجح الهاكر في إختراق النظام ولكن خلال أقل من خمس دقائق يستطيع موظفوا الشركة من إعادة الأمور إلى مجراها!!
- يعد الاختراق والتجسس جريمة يحاسب عليها القانون في الكثير من دول العالم ولذا لا تستغرب أخي الكريم أن ترى الهاكر بجوار القاتل ومروج المخدرات واللصوص ولكن الفرق أنه بمجرد خروج الهاكر من السجن يجد إستقبالاً حافلاً من الشركات العالمية الكبرى التي تسارع إلى توظيف الهاكرز بغرض الاستفادة من خبرتهم في محاربة الهاكرز وكذلك للاستفادة من معلوماتهم في بناء برامج وأنظمة يعجز الهاكرز عن إقتحامها

حكمة يؤمن بها كل الهاكرز : لا يوجد نظام تشغيل بدون منافذ ولا يوجد جهاز لا يحوي فجوة ولا يوجد جهاز لا يستطيع هاكر إقتحامه .

أغلب وأقوى الهاكر في العالم هم مبرمجوا الكمبيوتر ومهندسوا الاتصال والشبكات ولكن الأقوى منهم هم الشباب والمراهقون المتسلحون بالتحدي وروح المغامرة والذين يفرغون وقتهم لتعلم المزيد والمزيد في علم التجسس والتطفل على الناس ، وعموماً مصير كل هؤلاء في الغالب إلى السجن أو أكبر شركات الكمبيوتر والبرمجة في العالم !!

الآن تحولت الحروب من ساحات المعارك إلى ساحات الإنترنت والكمبيوتر

وأصبح الهاكرز من أقوى وأعتى الجنود الذين تستخدمهم الحكومات وخاصة المخابرات حيث يستطيعون التسلل بخفية إلى أجهزة وأنظمة العدو وسرقة معلومات لا تقدر بثمن وكذلك تدمير المواقع وغير ذلك .. وكذلك لا ننسى الحروب الإلكترونية التي تدور رحاها بين العرب واليهود والأمريكان والروس و... ربنا يحفظنا .

لمزيد من التواصل :

adlene@barcelona.net

